

This Page Is Inserted by IFW Operations
and is not a part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

**As rescanning documents *will not* correct images,
please do not report the images to the
Image Problem Mailbox.**

JP11032037
CERTIFICATION DATA GENERATING DEVICE
 FUJI XEROX CO LTD
 Inventor(s): NAKAGAKI JUHEI, SHIN YOSHIHIRO
 Application No. 09188801, Filed 19970714, Published 19990202

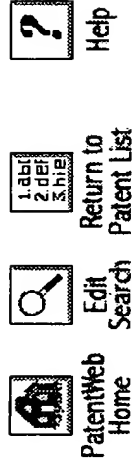
Abstract:

PROBLEM TO BE SOLVED: To pre-pay access qualification to purchase or rent without imposing any surplus load on a certification data generating device side.

SOLUTION: A pre-paid purchase ticket T_2 is stored in an access ticket storing part 13. Next, (T_1', n_2) is inputted to a certification data-inputting part 14. A use condition judging part 15 extracts a corresponding access ticket (t_2, L_2, n_2) , checks whether or not a use condition L_2 is fulfilled, and reduces frequency information V , when the use condition is fulfilled. A certification data generating and outputting part 16 calculates certification data R by using auxiliary certification decision $(t)_2$ and the use condition L_2 extracted by the use condition decision part 15 and (du) read from a user specific information storing part 11, and outputs T_1 . A user performs access to a program in a purchase state or a rent state by using the T_1 .

Int'l Class: H04L00932 G06F00906 G06F01500 G09C00100

MicroPat nt Reference Number: 000373409
 COPYRIGHT: (C) 1999 JPO



For further information, please contact:
[Technical Support](#) | [Billing](#) | [Sales](#) | [General Information](#)

(19)日本国特許庁 (J P)

(12) 公 開 特 許 公 報 (A)

(11)特許出願公開番号

特開平11-32037

(43)公開日 平成11年(1999)2月2日

(51)Int.Cl.⁶

識別記号

F I

H 0 4 L 9/32

H 0 4 L 9/00

6 7 5 B

G 0 6 F 9/06

G 0 6 F 9/06

5 5 0 Z

15/00

15/00

3 3 0 B

G 0 9 C 1/00

G 0 9 C 1/00

6 4 0 B

6 4 0 E

審査請求 未請求 請求項の数11 O L (全 18 頁)

(21)出願番号

特願平9-188801

(22)出願日

平成9年(1997)7月14日

(71)出願人 000005496

富士ゼロックス株式会社

東京都港区赤坂二丁目17番22号

(72)発明者 中垣 寿平

神奈川県足柄上郡中井町境430 グリーン

テクなかい 富士ゼロックス株式会社内

(72)発明者 申 吉浩

神奈川県足柄上郡中井町境430 グリーン

テクなかい 富士ゼロックス株式会社内

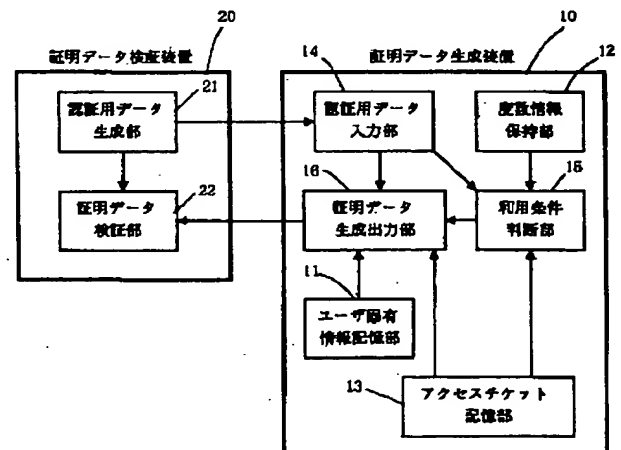
(74)代理人 弁理士 澤田 俊夫

(54)【発明の名称】 証明データ生成装置

(57)【要約】

【課題】 証明データ生成装置側に余分な負荷をかけることなく、買い取りやレントのアクセス資格をプリペイドで支払う。

【解決手段】 プリペイド払いバーチェス・チケットの T_2 はアクセスチケット記憶部 13 に格納される。次に、 (T_1', n_2) が認証用データ入力部 14 に入力される。利用条件判断部 15 は、対応するアクセスチケット (t_2, L_2, n_2) を取り出し、利用条件 L_2 が満たされるか調べ、満たされれば、度数情報 V を減額する。証明データ生成出力部 16 は、利用条件判断部 15 が取り出した証明用補助情報 t_2 、利用条件 L_2 と、ユーザ固有情報記憶部 11 から読み出した d_u とを用いて証明データ R を計算して T_1 を出力する。ユーザは T_1 を用いて買い取り状態であるいはレント状態でプログラムへのアクセスを行う。



実施例の構成図

【特許請求の範囲】

【請求項 1】 ユーザのアクセス資格を認証するために生成され、正当性を検証される証明データを生成する証明データ生成装置において、
認証用データを入力する認証用データ入力手段と、
ユーザの固有情報を記憶するユーザ固有情報記憶手段と、
ユーザの固有情報と、アクセス資格認証の特徴情報と、アクセス条件を記述した利用条件情報とに対し、所定の計算を実行して生成した証明用補助情報と、利用条件情報との組を含む証明用補助情報セットを記憶する証明用補助情報セット記憶手段と、
入力された認証用データに対応する証明用補助情報セットを上記証明用補助情報セット記憶手段から取り出し、上記取り出した証明用補助情報セットの利用条件情報に従い、以降の処理を継続するかどうかの判断を行う利用条件判断手段と上記利用条件判断手段において継続と判断されたときに、上記取り出した証明用補助情報セットと、上記認証用データ入力手段から入力された認証用データと、上記ユーザ固有情報記憶手段に記憶されている上記ユーザの固有情報とに所定の計算を施して証明データを生成し出力する証明データ生成出力手段とを有し、
上記認証用データ入力手段から、第 1 の証明用補助情報セットを暗号関数における暗号化鍵で暗号化した暗号化証明用補助情報セットを入力し、
上記利用条件判断手段は、上記証明用補助情報セット記憶手段から、入力された暗号化証明用補助情報セットに対応する第 2 の証明用補助情報セットを取り出し、上記取り出した第 2 の証明用補助情報セットの利用条件情報に従い、所定の処理を行った後、以降の処理を継続するかどうかの判断を行い、
上記証明データ生成出力手段は、上記処理を行うことにより、上記暗号化証明用補助情報セットを復号化した結果である第 1 の証明用補助情報セットを出力することを特徴とする証明データ生成装置。

【請求項 2】 少なくとも、上記ユーザ固有情報記憶手段と、上記利用条件判断手段と、上記証明データ生成出力手段とが、内部のデータおよび処理手続きを外部から観測することを困難ならしめる防御手段中に保持されている請求項 1 記載の証明データ生成装置。

【請求項 3】 さらに電子度数情報を保持する度数情報保持手段を備え、上記利用条件情報には、利用したときに支払うべき利用度数を含み、上記利用条件判断手段は、上記度数情報保持手段に保持されている電子度数情報と、上記利用条件情報に含まれる利用度数とを比較して、上記度数情報保持手段に保持されている電子度数情報が利用条件情報に含まれる利用度数以上の時のみ、上記度数情報保持手段に保持されている電子度数情報から上記利用条件情報に含まれる利用度数分の度数を減額して、以降の処理を継続するという判断を行う請求項 1

または 2 記載の証明データ生成装置。

【請求項 4】 上記第 1 の証明用補助情報セットに含まれる第 1 の利用条件情報に含まれる利用度数は 0 度数であり、上記第 2 の証明用補助情報セットに含まれる第 2 の利用条件情報に含まれる利用度数は 0 以外であることを特徴とする請求項 3 記載の証明データ生成装置。

【請求項 5】 さらに時刻を示す時計を備え、上記第 1 の証明用補助情報セットに含まれる第 1 の利用条件情報には、さらに有効期限情報が記載され、上記利用条件判断手段は、上記時刻と上記有効期限情報とを比較し、該時刻が有効期限内にある時のみ、以降の処理を継続するという判断を行う請求項 1、2、3 または 4 記載の証明データ生成装置。

【請求項 6】 少なくとも、上記証明用補助情報セット記憶手段以外の手段が、携帯可能な小型演算装置として構成されている請求項 1、2、3、4 または 5 記載の証明データ生成装置。

【請求項 7】 ユーザのアクセス資格を証明するために生成された証明データの正当性を検証することにより上記ユーザのアクセス資格を認証するアクセス資格認証装置において、

認証用データを記憶する第 1 の記憶手段と、

ユーザの固有情報を記憶する第 2 の記憶手段と、

上記ユーザの固有情報と、アクセス資格認証の特徴情報とに対して所定の計算を実行して生成した第 1 の証明用補助情報を暗号化して生成した暗号化証明用補助情報を記憶する第 3 の記憶手段と、

上記ユーザの固有情報と、上記暗号化の復号鍵と、アクセス条件を記述した利用条件情報とに対して、所定の計算を実行して生成した第 2 の証明用補助情報と、上記利用条件情報とからなる第 2 の証明用補助情報セットを記憶する第 4 の記憶手段と、

上記第 4 の記憶手段に記憶されている上記第 2 の証明用補助情報セットに含まれる上記利用条件情報にしたがって所定の処理を継続するかどうかを判断する手段と、

上記所定の処理を継続すると判断したときに、上記第 3 の記憶手段に記憶されている上記暗号化証明用補助情報と、上記第 2 の記憶手段に記憶されている上記ユーザの固有情報と、上記第 4 の記憶手段に記憶されている上記第 2 の証明用補助情報セットとに対して所定の計算を実行して上記第 1 の証明用補助情報を復元する手段と、

上記第 1 の記憶手段に記憶されている上記認証用データと、上記第 2 の記憶手段に記憶されている上記ユーザの固有情報と、復元した上記第 1 の認証用補助情報とに対して所定の計算を実行して証明データを生成する手段と、

生成された上記証明データを検証する手段とを有することを特徴とするアクセス資格認証装置。

【請求項 8】 ユーザのアクセス資格を証明するために生成された証明データの正当性を検証することにより上

記ユーザのアクセス資格を認証するアクセス資格認証装置において、

認証用データを記憶する第 1 の記憶手段と、
ユーザの固有情報を記憶する第 2 の記憶手段と、
上記ユーザの固有情報と、アクセス資格認証の特徴情報と、アクセス条件を記述した第 1 の利用条件情報とに対し、所定の計算を実行して生成した第 1 の証明用補助情報と、上記第 1 の利用条件情報とからなる第 1 の証明用補助情報セットを暗号化して生成した暗号化証明用補助情報セットを記憶する第 3 の記憶手段と、
上記ユーザの固有情報と、上記暗号化の復号鍵と、アクセス条件を記述した第 2 の利用条件情報とに対して、所定の計算を実行して生成した第 2 の証明用補助情報と、上記第 2 の利用条件情報とからなる第 2 の証明用補助情報セットを記憶する第 4 の記憶手段と、
上記第 4 の記憶手段に記憶されている上記第 2 の証明用補助情報セットに含まれる上記第 2 の利用条件情報にしたがって第 1 の処理を継続するかどうかを判断する手段と、

上記第 1 の処理を継続すると判断したときに、上記第 3 の記憶手段に記憶されている上記暗号化証明用補助情報セットと、上記第 2 の記憶手段に記憶されている上記ユーザの固有情報と、上記第 4 の記憶手段に記憶されている上記第 2 の証明用補助情報セットとに対して所定の計算を実行して上記第 1 の証明用補助情報セットを復元する手段と、

復元された上記第 1 の証明用補助情報セットに含まれる上記第 1 の利用条件情報にしたがって第 2 の処理を継続するかどうかを判断する手段と、

上記第 2 の処理を継続すると判断したときに、上記第 1 の記憶手段に記憶されている上記認証用データと、上記第 2 の記憶手段に記憶されている上記ユーザの固有情報と、復元した上記第 1 の証明用補助情報セットとに対して所定の計算を実行して証明データを生成する手段と、生成された上記証明データを検証する手段とを有することを特徴とするアクセス資格認証装置。

【請求項 9】 ユーザのアクセス資格を証明するために生成された証明データの正当性を検証することにより上記ユーザのアクセス資格を認証するアクセス資格認証方法において、

認証用データを記憶する第 1 のステップと、
ユーザの固有情報を記憶する第 2 の記憶ステップと、
上記ユーザの固有情報と、アクセス資格認証の特徴情報と、アクセス条件を記述した第 1 の利用条件情報とに対し、所定の計算を実行して生成した第 1 の証明用補助情報と、上記第 1 の利用条件情報とからなる第 1 の証明用補助情報セットを暗号化して生成した暗号化証明用補助情報セットを記憶する第 3 のステップと、
上記ユーザの固有情報と、上記暗号化の復号鍵と、アクセス条件を記述した第 2 の利用条件情報とに対して、所

定の計算を実行して生成した第 2 の証明用補助情報と、
上記第 2 の利用条件情報とからなる第 2 の証明用補助情報セットを記憶する第 4 の記憶ステップと、

上記第 4 の記憶ステップで記憶された上記第 2 の証明用補助情報セットに含まれる上記第 2 の利用条件情報にしたがって第 1 の処理を継続するかどうかを判断するステップと、

上記第 1 の処理を継続すると判断したときに、上記第 3 の記憶ステップで記憶された上記暗号化証明用補助情報セットと、上記第 1 の記憶ステップで記憶された上記ユーザの固有情報と、上記第 4 の記憶ステップで記憶された上記第 2 の証明用補助情報セットとに対して所定の計算を実行して上記第 1 の証明用補助情報セットを復元するステップと、

復元された上記第 1 の証明用補助情報セットに含まれる上記第 1 の利用条件情報にしたがって第 2 の処理を継続するかどうかを判断するステップと、

上記第 2 の処理を継続すると判断したときに、上記第 1 の記憶ステップで記憶された上記認証用データと、上記第 2 の記憶ステップで記憶された上記ユーザの固有情報と、復元した上記第 1 の証明用補助情報セットとに対して所定の計算を実行して証明データを生成するステップと、

生成された上記証明データを検証するステップとを有することを特徴とするアクセス資格認証方法。

【請求項 10】 ユーザのアクセス資格を証明するために生成された証明データの正当性を検証することにより上記ユーザのアクセス資格を認証するアクセス資格認証装置に用いる証明用補助情報を生成する証明用補助情報生成装置において、

ユーザの固有情報と、アクセス資格認証の特徴情報と、アクセス条件を記述した第 1 の利用条件情報とに対し、所定の計算を実行して第 1 の証明用補助情報を生成する手段と、

上記第 1 の証明用補助情報と、上記第 1 の利用条件情報とからなる第 1 の証明用補助情報セットを暗号化する手段と、

上記ユーザの固有情報と、上記暗号化の復号鍵と、アクセス条件を記述した第 2 の利用条件情報とに対して、所定の計算を実行して第 2 の証明用補助情報を生成する手段と、

上記暗号化した第 1 の証明用補助情報セットと上記第 2 の証明用補助情報セットとから複合的な証明用補助情報を生成して出力する手段とを有することを特徴とする証明用補助情報生成装置。

【請求項 11】 ユーザのアクセス資格を証明するために生成された証明データの正当性を検証することにより上記ユーザのアクセス資格を認証するアクセス資格認証装置に用いる証明用補助情報を生成する証明用補助情報生成方法において、

ユーザの固有情報と、アクセス資格認証の特徴情報と、アクセス条件を記述した第1の利用条件情報とに対し、所定の計算を実行して第1の証明用補助情報を生成するステップと、

上記第1の証明用補助情報と、上記第1の利用条件情報とからなる第1の証明用補助情報セットを暗号化するステップと、

上記ユーザの固有情報と、上記暗号化の復号鍵と、アクセス条件を記述した第2の利用条件情報とに対して、所定の計算を実行して第2の証明用補助情報を生成するステップとを有することを特徴とする証明用補助情報生成方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、ユーザの権限を証明するために生成された証明データの正当性を検証することによりユーザのアクセス資格を認証する技術に関し、とくに上記証明データを生成する証明データ生成装置に関するものである。

【0002】

【従来の技術】本発明と同分野に属する先行技術としてプログラムの実行制御技術が知られている。プログラム実行制御技術は、

①アプリケーションプログラム中にユーザ認証のためのルーチンを埋め込み、②該ルーチンはアプリケーションの実行を試みているユーザが正規の認証用の鍵を保有していることを検査し、

③前記認証用の鍵の存在が確認された場合に限りプログラムを続行し、それ以外の場合にはプログラムの実行を停止する技術である。

【0003】このような技術を利用することにより、認証鍵を保有する正規のユーザにのみアプリケーションプログラムの実行を可能ならしめることが出来る。当技術はソフトウェア頒布事業において実用化されており、製品として、例えばRainbow Technologies, Inc. 社のSentinel Super Pro (商標)や、Aladdin Knowledge Systems Ltd. 社のHASP (商標)等がある。

【0004】これらの技術では、ユーザの認証鍵は、ソフトウェアベンダが、複製を防ぐためにハードウェア中のメモリに厳重に封入し、郵便などの物理的手段を用いてユーザに配布し、ユーザはこれを所有のパソコンなどに装着して利用する。

【0005】これらの技術は、アプリケーションプログラムを作成する際に、プログラム作成者がユーザが持つ認証鍵を予め想定した上で、該認証鍵に基づいてプログラムの保護処理を行わなければならない。つまり、プログラム作成者は、鍵内蔵ハードウェアからの正しい返信をプログラム作成時に予測して、正しい返信を受けた場

合にのみプログラムが正常に動作するようにプログラムの作成を行わなければならない。

【0006】このような特徴を有する従来技術の利用形態は、基本的に以下の2通りとなる。

【0007】①第1の方法では、ユーザの認証鍵をユーザ毎に異なるように用意する。即ち、ユーザ甲には認証鍵甲、ユーザ乙には認証鍵乙というように、ユーザ毎に異なる認証鍵を一つずつ用意する。

【0008】②第2の方法では、プログラム作成者はアプリケーション毎にそれぞれ異なる認証鍵を用意する。即ち、アプリケーション甲には認証鍵甲、アプリケーション乙には認証鍵乙というように、アプリケーション毎に異なる認証鍵を一つずつ用意し、固有の認証鍵を識別するように各アプリケーションプログラムを作成する。

【0009】しかし、これらのいずれの場合にも、以下に述べるような問題を有する。

【0010】第1の方法の場合、プログラム作成者は、プログラム中の認証ルーチンをユーザ毎に適切に変えてプログラムを作成する必要がある。つまり、ユーザ毎に認証鍵が異なるので、プログラム中の認証ルーチンは該プログラムを利用するユーザ固有の認証鍵を識別するように作成されなければならない、プログラム作成者は利用ユーザの数だけ異なるプログラムを作成する必要がある。

【0011】対象となるユーザが多数の場合、プログラムをユーザ毎に個別化する作業はプログラム作成者にとって耐えがたい労力を要求し、管理しなければならないユーザ認証鍵のリストも膨大なものとなる。

【0012】第2の方法の場合、第1の方法の場合のようにユーザ毎にプログラムを個別的に作成する必要はなくなるが、逆に、ユーザは利用するアプリケーションの数だけ認証鍵を保持しなければならないこととなる。

【0013】この制約はプログラム作成者及びユーザそれぞれに以下のような問題を惹起する。

【0014】前述のように、認証鍵はハードウェアに厳重に封入した状態でユーザに配布する必要がある。従って、プログラム自身はネットワークを介して簡便に配布することができるのと対照的に、認証鍵を内蔵するハードウェアの配布は郵便等の物理手段に頼らざるを得ない。この制限は、コスト、時間、梱包の手間いずれをとっても、プログラム作成者にとって大きな負担となる。

【0015】プログラム作成者は、ユーザの要求に応えるべく、アプリケーション毎に異なるハードウェアを一定個数ストックしておかなければならず、在庫管理のコストを必要とする。

【0016】また、ユーザは利用するアプリケーションを変更する度にハードウェアを交換しなければならないという煩雑さに甘んじなければならない。

【0017】ユーザがあるアプリケーションを使いたいとしても、認証鍵が封入されたハードウェアが届くまで

待たねばならず、即座に利用できないという点での不便さも生ずる。

【0018】この問題を解決する技術として、本出願人は新たなアクセス資格検証手法を提案している（特願平08-062076号、現在未公開）。

【0019】特願平08-062076号の提案では、証明用補助情報（アクセスチケット）を導入することにより、アクセス資格認証の特徴情報とユーザ固有情報とを独立させ、プロテクト側も、ユーザ側も1つの固有情報を準備しておけばすむようにしている。

【0020】アクセスチケットは、特定のユーザの固有情報とアクセス資格認証の特徴情報とに基づいて計算されるデータであり、また、ユーザ固有情報を知らずに、アクセスチケットからアクセス資格認証の特徴情報を計算することは困難である。そして、ユーザ固有情報とアクセスチケットとの正しい組み合わせ、すなわち、ユーザ固有情報と該ユーザ固有情報に基づいて計算されたアクセスチケットの組み合わせが入力された場合に限り、正しい証明用データが計算される。

【0021】したがってユーザはあらかじめ固有情報を保持し、プログラム作成者等のプロテクト者はユーザが所持する固有情報とは独立にアクセス資格認証の特徴情報を用意し、アクセスチケットをユーザの固有情報とアプリケーションプログラムの作成等に使用したアクセス資格認証の特徴情報とに応じて作成し、配布することにより、実行制御等のユーザのアクセス資格の認証を行う事ができる。

【0022】この技術を用いて、アプリケーションプログラムにプロテクトを行ってユーザに配布し、アプリケーションプログラムの利用を希望するユーザに、アクセスチケットを提供するサービスが考えられる。

【0023】希望するユーザに、ユーザ毎に異なる固有情報を封入したICカードなどの媒体を渡しておき、またプログラム作成者はアクセス資格認証の特徴情報を用いてプログラムにプロテクトをかけて配布し、プログラムの利用を希望するユーザに、プログラム作成者またはプログラム作成者から委託を受けたチケット発行業者がアクセスチケットを提供する。

【0024】このようなサービスを考えた場合、いつどのようにして課金するかということが問題になる。この例の場合では、アクセスチケットを発行する際に、チケットの発行と引換えにプログラムの代金に相当する料金を徴収することができる。

【0025】ところで、このようなプログラムの利用権の売買サービスを考える場合、以下のような権利の形態が考えられる。

①パーチェス（purchase）：利用権を買いとってしまう方法。一度購入すると、永久に利用することができる。その後、利用する、しないにかかわらず、料金は同じである。

②ペイ・パー・ユース（pay-per-use）：利用量課金とも呼ばれる。利用した量に応じて課金される。

③レント（rent）：一定期間の利用権を購入する。期限が過ぎれば利用できなくなる。

【0026】前述の特願平08-062076号の技術を用いた場合、パーチェスを実現することは容易であるが、レントを実現するのは困難である。

【0027】ペイ・パー・ユースについては、利用する度毎にユーザが利用希望をチケット発行業者へ提出し、チケット発行業者は1回のみ使用可能なアクセスチケットを発行することにより実現することが可能であるが、頻繁にチケット発行操作が必要になる上に、1回のみ使用可能なアクセスチケットを実現するために、ユーザのICカード中に使用したチケットに対するログを記録していく必要があるため、あまり現実的ではない。

【0028】この問題に対しては、本出願人は利用制御情報をアクセスチケットの資格認証手法に導入することを提案している（特願平08-191756号、現在未公開）。特願平08-191756号の手法では、特願平08-062076号に利用制御情報を導入し、情報を復号化する際に、この利用制御情報も用いるものである。利用制御情報の例としては、使用期限、使用可能回数、総使用可能時間、使用上限金額、処理の履歴を取るか否かの情報などが記載されている。

【0029】利用制御情報が使用期限の場合には、レントを実現することが可能である。

【0030】また利用制御情報が処理の履歴を取るといった情報の場合には、一定期間後にその履歴を回収して集計することにより、利用した回数を計算し課金するという方法で、ペイ・パー・ユースに近い機能を実現することができる。さらに利用制御情報に1回あたりの利用額を記載するようにすれば、柔軟なペイ・パー・ユースを実現することが可能になる。

【0031】つまり特願平08-191756号の手法では、前述した権利の形態パーチェス、ペイ・パー・ユースおよびレントを全部実現できることになる。

【0032】次に、支払の方法について考える。支払の方法としては、以下の2つが考えられる。

【0033】①チケット発行時に支払う方法：チケット発行業者がアクセスチケットを発行する際に、支払う方法。電子貨幣により支払う場合や、発行業者側で料金を記録し、銀行振り込みなどにより清算を行う場合などがある。

【0034】②プリペイドで支払う方法：ユーザが予めプリペイド度数を購入して、ICカード中などに保持しておき、購入の際や利用の際に、プリペイドから相当する度数を引き落とす。

【0035】特願平08-191756号の技術を用いると、①チケット発行時に支払う方法で、前述した権利

の形態パーチェス、ペイ・パー・ユースおよびレントを全部実現できる。

【0036】他方、②プリペイドで支払う方法では、ペイ・パー・ユースは容易に実現できる。つまり、利用制御情報に1回あたりの利用額を記載し、認証を行う度に、保持しているプリペイド情報から、利用制御情報記載の度数分ずつ引き落とせばよい。

【0037】しかし、②プリペイドで支払う方法で、パーチェスやレントを実現するのは困難である。パーチェスは最初の利用時にのみプリペイドによる課金を行い、2回目以降の利用時には課金を行わないという処理が必要なためである。

【0038】パーチェスに関しては、利用制御情報に利用権の買取り額を記載しておき、最初の利用時にその額を保持しているプリペイド情報から引き落として、該利用したアクセスチケットの情報をICカードに登録するようにし、2回目以降の利用時には、利用しようとするチケットが既にICカードに登録されているかをチェックして、登録されている時にはプリペイド情報から引き落とさないように構成することで実現することも可能ではある。しかし、この登録情報は、非常に長い期間消すことはできないので、多くのチケットを使うような場合には、ICカードの記憶容量が不足することになり、あまり現実的な解決策ではない。

【0039】レントの場合も、利用制御情報にレンタル額と有効期限を記載しておき、パーチェスと同様の方法を取ることで、実現することは可能ではあるが、同じくICカードの記憶容量が不足することになり、あまり現実的な解決策ではない。

【0040】

【発明が解決しようとする課題】本発明は、以上のような問題点に鑑みなされたものであり、プリペイドで支払う方法においても、証明データ生成装置（ICカード）側に余分な負荷をかけることなく、パーチェスやレントを実現することを可能にすることを課題とする。

【0041】

【課題を解決するための手段】本発明によれば、上述の課題を解決するために、ユーザのアクセス資格を認証するために生成され、正当性を検証される証明データを生成する証明データ生成装置に、認証用データを入力する認証用データ入力手段と、ユーザの固有情報を記憶するユーザ固有情報記憶手段と、ユーザの固有情報と、アクセス資格認証の特徴情報と、アクセス条件を記述した利用条件情報とに対し、所定の計算を実行して生成した証明用補助情報と、利用条件情報との組を含む証明用補助情報セットを記憶する証明用補助情報セット記憶手段と、入力された認証用データに対応する証明用補助情報セットを上記証明用補助情報セット記憶手段から取り出し、上記取り出した証明用補助情報セットの利用条件情報に従い、以降の処理を継続するかどうかの判断を行う

利用条件判断手段と、上記利用条件判断手段において継続と判断されたときに、上記取り出した証明用補助情報セットと、上記認証用データ入力手段から入力された認証用データと、上記ユーザ固有情報記憶手段に記憶されている上記ユーザの固有情報とに所定の計算を施して証明データを生成し出力する証明データ生成出力手段とを設け、上記認証用データ入力手段から、第1の証明用補助情報セットを暗号関数における暗号化鍵で暗号化した暗号化証明用補助情報セットを入力し、上記利用条件判断手段は、上記証明用補助情報セット記憶手段から、入力された暗号化証明用補助情報セットに対応する第2の証明用補助情報セットを取り出し、上記取り出した第2の証明用補助情報セットの利用条件情報に従い、所定の処理を行った後、以降の処理を継続するかどうかの判断を行い、上記証明データ生成出力手段は、上記処理を行うことにより、上記暗号化証明用補助情報セットを復号化した結果である第1の証明用補助情報セットを出力するようにしている。

【0042】つまり、通常の証明用補助情報セット（アクセスチケット）である第1の証明用補助情報セットを暗号化して暗号化証明用補助情報セットを作成しておき、この暗号化証明用補助情報セットへアクセスするための第2の証明用補助情報セットを用いて、通常の認証処理と全く同じ処理を行うことにより、暗号化証明用補助情報セットから、第1の証明用補助情報セットを復号化する。

【0043】このように構成することにより、利用料金が無料のチケット（第1の証明用補助情報セット）を作成して暗号化し、暗号化されたチケットを復号化するためのチケット（第2の証明用補助情報セット）を発行し、このチケット（第2の証明用補助情報セット）の利用料金を有料としプリペイドで支払うように構成することで、全体としてプリペイドにおけるパーチェス機能の実現を可能にする。

【0044】レント機能は、これに加えて第2の証明用補助情報セットの利用条件情報に有効期限情報を記載することで実現可能である。

【0045】なお、暗号化されたチケットを復号化するには、通常のチケットの認証処理と同じ処理を行うように構成したので、比較的容量の少ないICカード内に、余分なプログラムやデータを入れることなく、効率的に実現することが可能である。

【0046】

【発明の実施の形態】以下、この発明の実施例について説明する。

【0047】図1はこの実施例の構成図を示す。この実施例では、証明データ生成装置内にプリペイド情報を保持し、そのプリペイド情報を用いて、アプリケーションプログラムのアクセス権を購入する例（パーチェス）について説明する。

【0048】図1では、証明データ生成装置で生成され出力された証明データを検証する証明データ検証装置を含めて示す。

【0049】まず、図1に基づいて、本実施例の構成について説明したあと、証明データ検証装置、証明データ生成装置の処理の流れをフローチャートで示しながら説明する。処理の流れの説明には、通常の認証処理を例にして説明し、利用条件情報Lには、1回の利用の度ごとにプリペイドから引き落とされる例について説明する。そして、通常の認証処理の説明の後に、アプリケーションプログラムのアクセス権を購入する例（パーチェス）について説明する。

【0050】〔実施例の構成〕図1は実施例の構成を全体として示すものであり、この図において、証明データ生成装置10はユーザが保持するものであり、例えばICカードのように内部に計算機能を持った携帯型の装置である。ICカード以外にも、計算機能を持ったPCカードや、携帯型情報ツール、あるいはサブノートパソコンなどでもよい。内部の情報が、外部から簡単に改竄されたりすることがないように防御されていることが望ましい。

【0051】証明データ検証装置20はユーザがアプリケーションプログラムを使用するパソコンであり、パソコンのスロットに証明データ生成装置10であるICカードを装着して使用する。

【0052】証明データ検証装置20は、大きく認証用データ生成部21と証明データ検証部22とから構成されている。認証用データ生成部21は、認証が必要な時に、認証用データを生成して、証明データ生成装置10に送付する。証明データ検証部22は、証明データ生成装置10から送り返された証明データが正しいかどうかを検証する。

【0053】アプリケーションプログラムは、暗号化などによりプロテクトされており、ユーザがアプリケーションプログラムを利用しようとする、証明データ検証装置20は、そのアプリケーションプログラムに対応した認証用データを作成し、証明データ生成装置10に送り、証明データ生成装置10から送り返された証明データを検証して、正しいと検証された場合に限り、アプリケーションプログラムのプロテクトを解除して、利用することを可能にする。

【0054】一方、証明データ生成装置10は、ユーザ固有情報記憶部11、度数情報保持部12、アクセスチケット記憶部13、認証用データ入力部14、利用条件判断部15、証明データ生成出力部16を含んで構成される。

【0055】ユーザ固有情報記憶部11は、ユーザの秘密情報を保持する部分であり、ユーザ毎に異なる情報である。ユーザ固有情報は、証明データ生成装置10が作成された時に封入され、ユーザにも取り出せないように

構成されていることが望ましい。

【0056】度数情報保持部12は、プリペイド情報を保持する部分であり、アプリケーションプログラムの利用や購入などに応じて、必要な額が減額されていく。額が少なくなった時には、増額することも可能である。増額の方法は、例えば、特願平9-21373号で提案されている手法を用いることができる。この手法では、度数情報と署名した度数情報とを用いて度数情報を増額する。度数情報保持部12における額の増減は、安全に行われることが必要であり、定められた方法以外でのアクセスができないように構成することが望ましい。

【0057】アクセスチケット記憶部13は、複数のアクセスチケットを記憶している。アクセスチケットは、ユーザにアクセス資格を与えるものであり、アプリケーションプログラム作成者、またはアプリケーションプログラム作成者から委託を受けたチケット発行業者によって作成される。本実施例では、アクセスチケットは、ユーザの固有情報と、アクセス資格認証の特徴情報と、アクセス資格認証のアクセス条件を記述した利用条件情報とに対し、所定の計算を実行して計算された証明用補助情報と利用条件情報との組である。本実施例では、アクセスチケット記憶部は、ICカード中に構成されているが、アクセスチケットは発行された本人しか使えないため、コピーは自由であり、ICカード外部に構成しても構わない。

【0058】認証用データ入力部14は、証明データ検証装置20から送られた認証用データを入力する部分である。

【0059】利用条件判断部15は、入力された認証用データに対応するアクセスチケットをアクセスチケット記憶部13から取り出し、アクセスチケット中の利用条件情報を元に、利用条件を判断する。例えば、アクセスチケットの有効期限が切れていないか、利用料金は保持しているプリペイドで支払うのに足りているか、などの利用条件を判断し、以降の処理を継続するか否かを判断する。

【0060】証明データ生成出力部16は、利用条件判断部15で継続と判断された時のみ、証明データを生成して出力する。証明データは、利用条件判断部15で取り出したアクセスチケット中の証明用補助情報と、認証用データと、ユーザの固有情報とに所定の計算を施して作成する。

【0061】次に、具体例を挙げて、さらに詳細に説明する。ここでの説明は、通常の認証処理を例にして説明し、利用条件情報Lには、1回の利用の度ごとにプリペイドから引き落とされる例について説明する。

【0062】図2は、図1の構成図に記号を付けたものである。記号は以下の説明と対応している。

【0063】〔通常の認証処理〕以下では、法nにおけるRSA (R i v e s t - S h a m i r - A d e l m a

n) 暗号を用いた例について詳細に説明する。まず、通常の認証処理について説明する。以下の例では、アプリケーションプログラムの作成者であるソフトウェアベンダが、ICカードの発行からチケットの発行まですべてを行う例について説明する。この例ではソフトウェアベンダは、すべてのユーザの秘密情報 d_u を知っている。これ以外にも、ICカードの発行とチケットとをチケット発行業者が行う構成も可能である。

【0064】ソフトウェアベンダは、プロテクトしたいアプリケーションプログラムに対する暗号鍵を作成する。ここではRSA暗号を用いるので、大きな素数 p 、 q を秘密に作成し、法数 n を $n = p \cdot q$ として作成する。次に法数 n の元で暗号鍵 E と復号鍵 D を、

【0065】

【数1】 $ED \equiv 1 \pmod{\phi(n)}$

を満たすように生成する。ここで $\phi(n)$ はオイラー数であり、 $\phi(n) = (p-1)(q-1)$ である。

【0066】次にソフトウェアベンダは、共通暗号鍵 K を作り、プロテクトしたいアプリケーションプログラムの一部または全部を、 K で暗号化し、

【0067】

【数2】 $K' = K^E \pmod{n}$

を計算して、 K' を暗号化したアプリケーションプログラムに、第3者が取り出せないように埋め込んで配布する。

【0068】このアプリケーションプログラムを利用したいユーザは、予めこれに対応するアクセスチケットを入手しておくことになる。

【0069】ソフトウェアベンダは、ユーザからのアクセスチケット発行要求を受けて、アクセスチケットを発行する。ソフトウェアベンダは、要求したユーザの秘密情報 d_u と、アプリケーションプログラムの暗号化の際に用いた暗号鍵 (E, n) に対応する復号鍵 (D, n) とをデータベースから取り出す。次にアクセスチケットに付与する利用条件情報 L を作成する。ここではプリペイドから引き落として課金するので、1回の利用について引き落とす利用額を L とする。そして、これらの情報を用いて、

【0070】

【数3】 $t = D - F(n, L, d_u)$

として証明用補助情報 t を作成する。ここで関数 $F()$ は一方向性の関数であり、一方向性ハッシュ関数MD5、SHAなどや、共通鍵暗号DES(Data Encryption Standard)などを用いることができる。

【0071】ソフトウェアベンダは、(t, L, n) の組をアクセスチケットとしてユーザに発行する。

【0072】ユーザが、アプリケーションプログラムを利用しようとする、証明データ検証装置は、そのアプリケーションプログラムに対応した認証用データ (C 、

n) を作成し、証明データ生成装置に送る。

【0073】この処理の流れを図3のフローチャートに示し、これに基づいて説明する。

(ステップS11) : 証明データ生成部21は、プロテクトされたアプリケーションプログラムから、 K' と n とを取り出す。

(ステップS12) : 証明データ生成部は、乱数 r を生成し、乱数保持部に格納する。

(ステップS13) : $C = r^E K' \pmod{n}$ を計算する。

(ステップS14) : (C, n) の組を認証用データとして証明データ生成装置10に送付する。

【0074】次に、証明データ生成装置10の流れを図4に示し、これに基づいて証明データ生成装置10の処理を説明する。

(ステップS21) : 認証用データ入力部14より、認証用データ (C, n) を入力する。

(ステップS22) : 利用条件判断部15は、 n をキーにしてアクセスチケット記憶部を検索し、アクセスチケット (t, L, n) を取り出す。

(ステップS23) : 利用条件判断部15は、取り出したアクセスチケット中の利用条件 L (利用額) と、度数情報保持部の度数情報 V とを比較する。

(ステップS24~S25) : $V \geq L$ の時は、証明データ生成出力部16は、(ステップS26)に進む。そうでないときは、証明データ生成出力部は、エラーを出力して終了する。

(ステップS26) : 利用条件判断部15は、度数情報保持部12に保持されている度数情報 V を利用条件 (利用額) L の分だけ減額する。

(ステップS26~S29) : 証明データ生成出力部16は、利用条件判断部15が取り出した証明用補助情報 t 、利用条件 L (利用額) と、ユーザ固有情報記憶部11から読み出した d_u とを用いて証明データ R を計算して出力する。

【0075】

【数4】 $R' = C^{F(n, L, d_u)} \pmod{n}$

$R = C \cdot R' \pmod{n}$

図4では、証明データ R を計算するのに、一旦 R' の計算を分けている。これは、 R' の計算にはユーザの秘密情報を用いるため、その処理が外部に漏れないように計算する必要があるが、一旦 R' の計算が終われば、 R の計算は外部で行っても構わないためである。このように R' と R とに分けて計算してもよいし、一度に計算しても構わない。

【0076】次に、証明データ検証装置20の証明データ検証部の処理について説明する。証明データ生成装置10から出力された証明データ R は、正しいユーザ固有情報 d_u と、正しいアクセスチケット (正しい証明用補助情報 t 、正しい利用条件 L) を用いて計算されたとき

には、

【0077】

【数5】

$$\begin{aligned} R &= C^{\dagger R'} \pmod n \\ &= C^{D \cdot F(n, L, du)} C^{F(n, L, du)} \pmod n \\ &= C^D \pmod n \\ &= (r^E K')^D \pmod n \\ &= (r^{EK^E})^D \pmod n \\ &= (rK)^{ED} \pmod n \\ &= rK \end{aligned}$$

となる。

【0078】そこで、証明データ検証部22では、乱数保持部23から乱数 r を取り出し、

【0079】

【数6】 $r^{-1}R \pmod n$

を計算することで、アプリケーションを暗号化していた共通暗号鍵 K を入手することができる。証明データ検証装置は、この共通暗号鍵 K でアプリケーションの暗号化されていた部分を復号し、アプリケーションを実行することができる。

【0080】この例では、証明データ検証装置は、アプリケーションが正しく実行できたことをもって、正しく検証ができたと判断する。

【0081】以上で通常の認証処理の説明を終了する。

【0082】[パーチェス] 次に、プリペイド情報を用いて、アプリケーションプログラムのアクセス権を購入する(パーチェス)例について説明する。

【0083】この機能を実現するには、通常のアクセスチケットである第1のアクセスチケットを暗号化して暗号化アクセスチケットを作成しておき、この暗号化アクセスチケットへアクセスするための第2のアクセスチケットを用いて、通常の認証処理と全く同じ処理を行うことにより、暗号化アクセスチケットから、第1のアクセスチケットを復号化する。

【0084】そしてこのとき、第1のアクセスチケットは、利用料金が無料のチケットとして作成し、第2のアクセスチケットは、利用料金を有料としプリペイドで支払うように構成することで、全体としてプリペイドにおけるパーチェス機能の実現を可能にする。

【0085】まず、パーチェスの機能を実現したいアプリケーションプログラムをAP1とする。上述の説明と同様に、AP1をプロテクトする。

【0086】<アプリケーションプログラムAP1のプロテクトの説明>ソフトウェアベンダは、プロテクトしたいアプリケーションプログラムに対する暗号鍵を作成する。ここではRSA暗号を用いるので、大きな素数 p_1 、 q_1 を秘密に作成し、法数 $n_1 = p_1 \cdot q_1$ として作成する。次に法数 n_1 の元で暗号鍵 E_1 と復号鍵 D_1 を、

【0087】

【数7】 $E_1 \cdot D_1 \equiv 1 \pmod{\phi(n_1)}$

を満たすように生成する。ここで $\phi(n_1)$ はオイラー数であり、 $\phi(n_1) = (p_1 - 1)(q_1 - 1)$ である。

【0088】次にソフトウェアベンダは、共通暗号鍵 K_1 を作り、プロテクトしたいアプリケーションプログラムの一部または全部を K_1 で暗号化し、さらに共通暗号鍵 K_1 を以下の式に従って、暗号鍵 E_1 で暗号化して、 K_1' を生成する。

【0089】

【数8】 $K_1' = K_1 E_1 \pmod{n_1}$

そして、 K_1' を暗号化したアプリケーションプログラムに、第3者が容易に取り出せないように埋め込んで配布する。また、 n_1 も、暗号化したアプリケーションプログラムに埋め込む。

【0090】ソフトウェアベンダは、作成した $(n_1, D_1, \phi(n_1))$ の組をアクセスチケット情報データベースに記憶する。

【0091】次に、プリペイド払いパーチェス・チケットの作成について説明する。図5は、証明用補助情報生成装置30の構成例を示したものである。この例では、第1の利用条件情報と第1の復号鍵とユーザ固有情報と第2の利用条件情報とを入力として、プリペイド払いパーチェス・チケットを出力する。図5において、入力部31は、第1の利用条件情報と第1の復号鍵とユーザ固有情報と第2の利用条件情報とを入力する部分である。第1復号鍵記憶部33は、入力部31から入力された第1の復号鍵を記憶する部分である。第1の復号鍵は、アプリケーションプログラムAP1の暗号化に用いた共通暗号鍵 K_1 を暗号化した暗号鍵 (E_1, n_1) に対応する復号鍵 (D_1, n_1) である。

【0092】ユーザ固有情報記憶部34は、入力部31から入力されたユーザ固有情報を記憶する部分である。これは、ユーザの証明データ生成装置10に格納されているものと同一のものである。

【0093】ユーザがチケットの発行を依頼する時には、ユーザの識別情報 U と、ユーザが利用を希望するアプリケーションプログラムAP1から取り出した n_1 とを、ソフトウェアベンダに送る。ソフトウェアベンダは、ユーザの識別情報 U とユーザ固有情報 du とを対応づけて保持しているユーザ情報データベースから、ユーザの識別情報 U に対応するユーザ固有情報 du を検索することによってユーザ固有情報を得、また $(n_1, D_1, \phi(n_1))$ の組を保持しているアクセスチケット情報データベースから、 n_1 に対応する復号鍵 (D_1, n_1) を得て、証明用補助情報生成装置30に入力する。

【0094】第1利用条件情報記憶部32と第2利用条件情報記憶部35は、それぞれ第1の利用条件情報と第2の利用条件情報とを記憶する部分である。第1の利用条件情報は、アプリケーションプログラムAP1の利用

条件を記述したものであり、第2の利用条件情報は、プリペイド払いパーチェス・チケットの利用条件を記述したものである。プリペイド払いパーチェス・チケットの場合には、1回目の利用時に課金され、2回目以降の利用時には課金されないという特性を持つので、第1の利用条件情報には少なくとも無料であることを意味する情報が含まれており、第2の利用条件情報には、少なくとも有料であることを意味する情報が含まれている。

【0095】第1チケット生成部36は、入力された第1の利用条件情報と第1の復号鍵とユーザ固有情報とに所定の計算を実行してアクセスチケットを生成する部分である。

【0096】第1利用条件情報記憶部32と第1復号鍵記憶部33とユーザ固有情報記憶部34と第1チケット生成部36とからなる構成部分41は、通常のアクセスチケットを生成するのと同様の構成をなしている。

【0097】第2の鍵生成部37は、第1チケット生成部36で生成された第1のアクセスチケットを暗号化するための鍵を生成する部分である。

【0098】暗号化部38は、第1チケット生成部36で生成された第1のアクセスチケットを、第2の鍵生成部37で生成された暗号化鍵を用いて暗号化する部分である。

【0099】第2チケット生成部39は、暗号化部38で暗号化された暗号化アクセスチケットを復号化するために必要となる第2のアクセスチケットを生成する部分である。

【0100】チケット出力部40は、暗号化部38で暗号化された暗号化アクセスチケットと、第2チケット生成部39で生成された第2のアクセスチケットとを組み合わせ、プリペイド払いパーチェス・チケットとして出力する。

【0101】<プリペイド払いパーチェス・チケットの作成>以下に、プリペイド払いパーチェス・チケットの作成の方法について図6のフローチャートを用いて説明する。

【0102】ソフトウェアベンダは、ユーザからのプリペイド払いパーチェス・チケット発行要求を受けて、プリペイド払いパーチェス・チケットを発行する。チケットの発行を依頼するユーザは、ユーザの識別情報Uと、ユーザが利用を希望するアプリケーションプログラムAP1から取り出した n_1 とを、ソフトウェアベンダに送る。

【0103】(ステップS31)：ソフトウェアベンダは、ユーザからのプリペイド払いパーチェス・チケット発行要求であるユーザの識別情報UとアプリケーションプログラムAP1から取り出した n_1 との組(U, n_1)を入力する。また、アプリケーションプログラムAP1の利用条件を記述した第1の利用条件情報 L_1 と、プリペイド払いパーチェス・チケットの利用条件を記述した

第2の利用条件情報 L_2 も入力する。ここでは、プリペイド払いパーチェス・チケットの生成を目的としているので、第1の利用条件情報 L_1 は、利用料金が無料であることを意味する

【0104】

【数9】 $L_1 = 0$

であり、第2の利用条件情報 L_2 は、パーチェスの料金が有料であることを意味する

【0105】

【数10】 $L_2 = A$

とする。ただしAは0以外の数字であり、たとえば100である。

【0106】(ステップS32)：ユーザの識別情報Uとユーザ固有情報duとを対応づけて保持しているユーザ情報データベースから、ユーザの識別情報Uに対応するユーザ固有情報duを検索する。

(ステップS33)：(n , D, $\phi(n)$)の組を保持しているアクセスチケット情報データベースから、 n_1 に対応する第1の復号鍵(D_1 , n_1)を検索する。

(ステップS34)：ユーザがAP1にアクセスするための第1のアクセスチケット T_1 を作成する。

【0107】

【数11】 $T_1 = (t_1, L_1, n_1)$

$t_1 = D_1 - F(n_1, L_1, du)$

(ステップS35)：第1のアクセスチケット T_1 を暗号化するために、第2の法数 n_2 、第2の暗号鍵 E_2 、第2の復号鍵 D_2 を生成する。大きな素数 p_2 , q_2 を生成し、以下の式が成り立つように、法数 n_2 、暗号鍵 E_2 、復号鍵 D_2 を生成する。

【0108】

【数12】 $n_2 = p_2 \cdot q_2$

$E_2 \cdot D_2 \equiv 1 \pmod{\phi(n_2)}$

$\phi(n_2) = (p_2 - 1)(q_2 - 1)$

(ステップS36)：生成した第2の暗号鍵 E_2 で第1のアクセスチケット T_1 を暗号化する。 T_1 を暗号化したものを T_1' とする。

【0109】

【数13】 $T_1' = T_1 E_2 \pmod{n_2}$

(ステップS37)：暗号化されたアクセスチケット T_1' をユーザが復号するための第2のアクセスチケット T_2 を作成する。

【0110】

【数14】 $T_2 = (t_2, L_2, n_2)$

$t_2 = D_2 - F(n_2, L_2, du)$

(ステップS38)：((T_1', n_2) , T_2)を組にしてプリペイド払いパーチェス・チケットとして出力する。

【0111】ソフトウェアベンダは、出力されたプリペイド払いパーチェス・チケット((T_1', n_2) , T_2)を、ユーザに送付する。

【0112】次に、プリペイド払いパーチェス・チケットの使用例について説明する。

【0113】<プリペイド払いパーチェス・チケットの使用例>

(a) プリペイド払いパーチェス・チケット

((T_1', n_2) , T_2)を受け取ったユーザは、まず T_2 をアクセスチケット記憶部 13 に格納する。

(b) 次に、(T_1' , n_2) を自分が保持している証明データ生成装置 10 の認証用データ入力部 14 より入力する。

【0114】以下、証明データ生成装置 10 における処理が図 4 に従って行われる。今、証明データ生成装置 14 の度数情報保持部 12 には、800 度数のプリペイド情報 V が保持されているとする。($V=800$)

(ステップ S 21) : 認証用データ入力部 14 より、認証用データ (T_1' , n_2) を入力する。

(ステップ S 22) : 利用条件判断部 15 は、 n_2 をキーにしてアクセスチケット記憶部 13 を検索し、アクセスチケット $T_2 = (t_2, L_2, n_2)$ を取り出す。

(ステップ S 23) : 利用条件判断部 15 は、取り出したアクセスチケット中の利用条件 L_2 と、度数情報保持部 12 の度数情報 V とを比較する。

(ステップ S 24) : 今、 $L_2=100$ 、 $V=800$ なので、

【0115】

【数 15】 $V \geq L_2$

が成り立ち、(ステップ S 26) へ進む。

(ステップ S 26) : 利用条件判断部 15 は、度数情報保持部 12 に保持されている度数情報 V を利用条件 L_2 の分だけ減額する。

【0116】

【数 16】 $V=800-100=700$

つまり、度数情報 V は、プリペイド払いパーチェス・チケットの買取り料金として、100 度数引き落とされ、残り 700 度数となる。

(ステップ S 27~S 29) : 証明データ生成出力部 16 は、利用条件判断部 15 が取り出した証明用補助情報 t_2 、利用条件 L_2 と、ユーザ固有情報記憶部 11 から読み出した du とを用いて証明データ R を計算して出力する。

【0117】

【数 17】 $R' = T_1' \cdot F(n_2, L_2, du) \mod n_2$

$R = T_1' \cdot R' \mod n_2$

R の計算を行うと、

【0118】

【数 18】

$R = T_1' \cdot R' \mod n_2$

$= T_1' \cdot {}^{D2-F(n_2, L_2, du)} C^{F(n_2, L_2, du)} \mod n_2$

$= T_1' \cdot {}^{D2} \mod n_2$

$= (T_1 \cdot {}^{E2})^{D2} \mod n_2$

$= T_1$

という計算が成り立ち、証明データ生成出力部 16 から、証明データ R として

【0119】

【数 19】 $R = T_1$

が出力される。

【0120】つまり、(T_1' , n_2) を自分が保持している証明データ生成装置 10 の認証用データ入力部 14 より入力すると、 L_2 が度数情報 V から引き落とされて、結果として T_1' が復号された T_1 が出力される。

【0121】(c) ユーザは、入手した T_1 をアクセスチケット記憶部 13 に格納する。

【0122】(d) ユーザは、アプリケーションプログラム AP1 を利用するためのアクセスチケット T_1 を入手できたので、アプリケーションプログラム AP1 を利用する。

【0123】以下、証明データ検証装置 10 における認証用データ生成処理が図 3 に従って行われる。

(ステップ S 11) : 認証用データ生成部 21 は、プロテクトされたアプリケーションプログラムから、 K_1' と n_1 とを取り出す。

(ステップ S 12) : 認証用データ生成部 21 は、乱数 r を生成し、乱数保持部 23 に格納する。

(ステップ S 13) : $C = r^E K_1' \mod n_1$ を計算する。

(ステップ S 14) : (C , n_1) の組を認証用データとして証明データ生成装置 10 に送付する。

(e) 証明データ生成装置 10 における処理が再び図 4 に従って行われる。

(ステップ S 21) : 認証用データ入力部 14 より、認証用データ (C , n_1) を入力する。

(ステップ S 22) : 利用条件判断部 15 は、 n_1 をキーにしてアクセスチケット記憶部 13 を検索し、アクセスチケット $T_1 = (t_1, L_1, n_1)$ を取り出す。

(ステップ S 23) : 利用条件判断部 15 は、取り出したアクセスチケット中の利用条件 L_1 と、度数情報保持部 12 の度数情報 V とを比較する。

(ステップ S 24) : 今、 $L_1=0$ 、 $V=700$ なので、

【0124】

【数 20】 $V \geq L_1$

が成り立ち、(ステップ S 26) へ進む。

(ステップ S 26) : 利用条件判断部 15 は、度数情報保持部 12 に保持されている度数情報 V を利用条件 L_1 の分だけ減額する。

【0125】

【数 21】 $V=700-0=700$

つまり、度数情報 V は、最初にプリペイド払いパーチェス・チケットの買取り料金として、100 度数引き落とされているので、2回目以降の利用では引き落とされ

ず、残り700度数のままとなる。

(ステップS27～S29)：証明データ生成出力部16は、利用条件判断部15が取り出した証明用補助情報 t_1 、利用条件 L_1 と、ユーザ固有情報記憶部11から読み出した du とを用いて証明データ R を計算して出力する。

【0126】

【数22】 $R' = C^{F(n_1, L_1, du)} \mod n_1$

$R = C^{-1}R' \mod n_1$

つまり、

【0127】

【数23】

$R = C^{-1}R' \mod n_1$

$= r^k$

(f) 証明データ検証装置20の証明データ検証部22は通常の認証と同様に処理を行い、乱数保持部23から乱数 r を取り出し、

【0128】

【数24】 $r^{-1}R \mod n_1$

を計算することで、アプリケーションを暗号化していた共通暗号鍵 K を入手することができる。証明データ検証装置は、この共通暗号鍵 K でアプリケーションの暗号化されていた部分を復号し、アプリケーションを実行することができる。

【0129】これ以降は、何度アプリケーションプログラムAP1を実行しても、同様の処理が行われ、無料で利用することができる。

【0130】以上説明したように、上記のように構成することで、プリペイド情報を用いて、アプリケーションプログラムのアクセス権を購入する(パーチェス)ことが可能になる。

【0131】以上、プリペイドにおけるパーチェス機能の実現について説明した。

【0132】これ以外にも、証明データ生成装置に時計を備え、第1のアクセスチケットの利用条件情報 L の中に、利用額が無料という情報に加えて、有効期限情報を記載し、第1のアクセスチケットの利用のたびに、時刻と比較することによって、プリペイドにおけるレント機能を実現することも可能である。

【0133】さらに、別の例としては、証明データ生成装置に時計を備え、第2のアクセスチケットの利用条件情報 L の中に、有効期限情報を記載し、暗号化された第1のアクセスチケットの復号の際に、時刻と比較することによって、第1のアクセスチケットを配布(解凍)する期限を限定することなども可能である。

【0134】また、本実施例では、RSA暗号を元にして説明を行ったが、これに限らず他の暗号方式を用いても構わない。また、アクセスチケットの実現式もこれに限ることはない。

【0135】

【発明の効果】実行制御等のユーザのアクセス資格の認証を行うに際して、ユーザはあらかじめ固有情報を保持し、プログラム作成者等のプロテクト者はユーザが所持する固有情報とは独立にアクセス資格認証の特徴情報を用意し、アクセスチケットをユーザの固有情報とアプリケーションプログラムの作成等に使用したアクセス資格認証の特徴情報とに応じて作成し、配布することにより、ユーザおよびプロテクト者の双方を、アクセス権情報管理のわずらわしさから開放させるという特徴を残したまま、従来は困難だったプリペイドにおけるパーチェス機能およびレント機能を実現することを可能にした。

【0136】さらにこれらの機能を実現するにおいて、通常のチケットの認証処理と同じ処理を行うように構成したので、比較的容量の少ないICカード内に、余分なプログラムやデータを入れることなく、効率的に実現することが可能である。

【図面の簡単な説明】

【図1】 本発明の実施例の構成を示すブロック図である。

【図2】 図1の構成を詳細に説明する図である。

【図3】 図1の証明データ検証装置の認証用データ生成処理を説明するフローチャートである。

【図4】 図1の証明データ生成装置の証明データ生成処理を説明するフローチャートである。

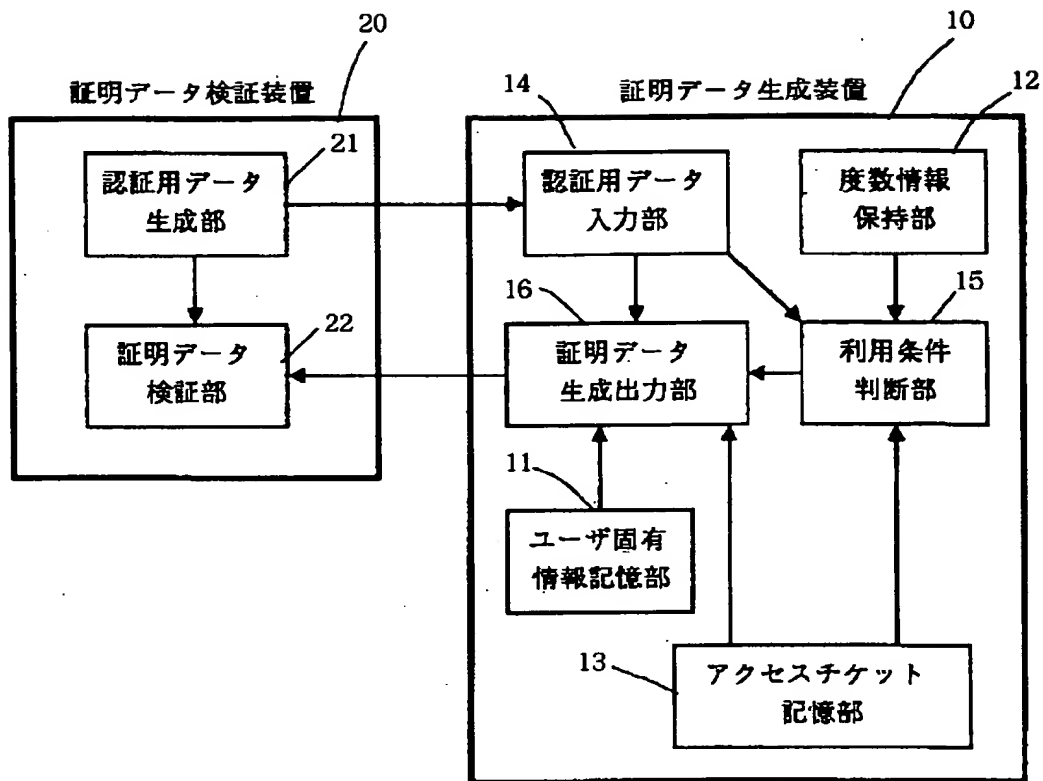
【図5】 図1の証明データの生成に用いるチケットを生成する証明用補助情報生成装置を示すブロック図である。

【図6】 図1の証明データの生成に用いるチケットの生成を説明する図である。

【符号の説明】

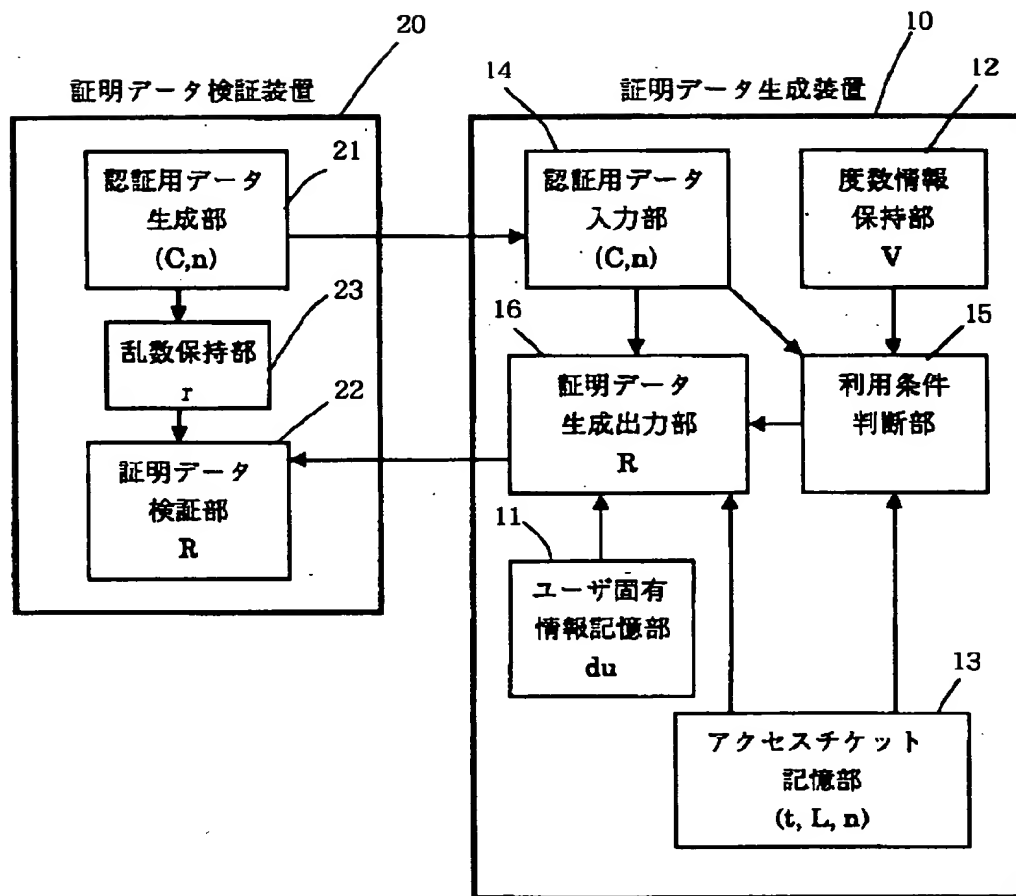
- 10 証明データ生成装置
- 11 ユーザ固有情報記憶部
- 12 度数情報保持部
- 13 アクセスチケット記憶部
- 14 認証用データ入力部
- 15 利用条件判断部
- 16 証明データ生成出力部
- 20 証明データ検証装置
- 21 認証用データ生成部
- 22 証明データ検証部
- 23 乱数保持部
- 30 証明用補助情報生成装置
- 32 第1利用条件情報記憶部
- 33 第1復号鍵記憶部
- 34 ユーザ固有情報記憶部
- 35 第2利用条件記憶部
- 36 第1チケット生成部
- 37 第2の鍵生成部
- 38 暗号化部
- 39 第2チケット生成部

【図 1】



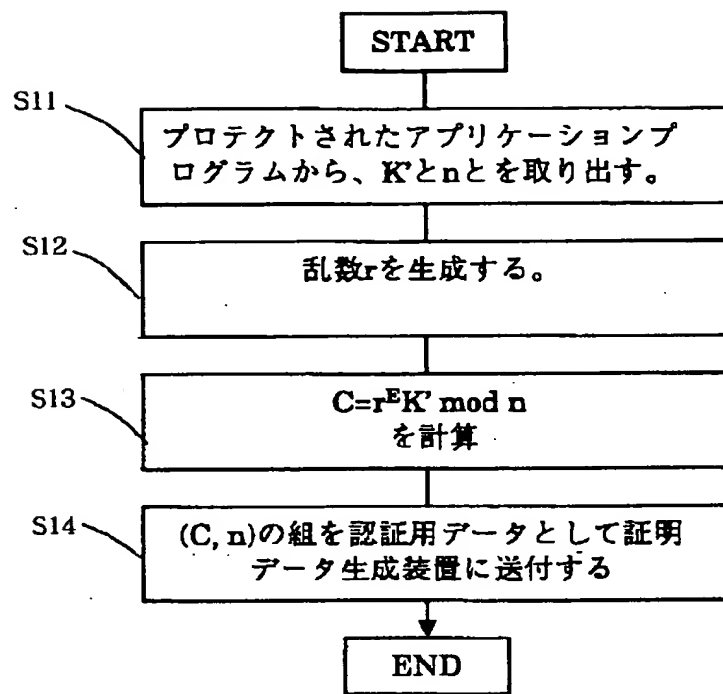
実施例の構成図

【図 2】



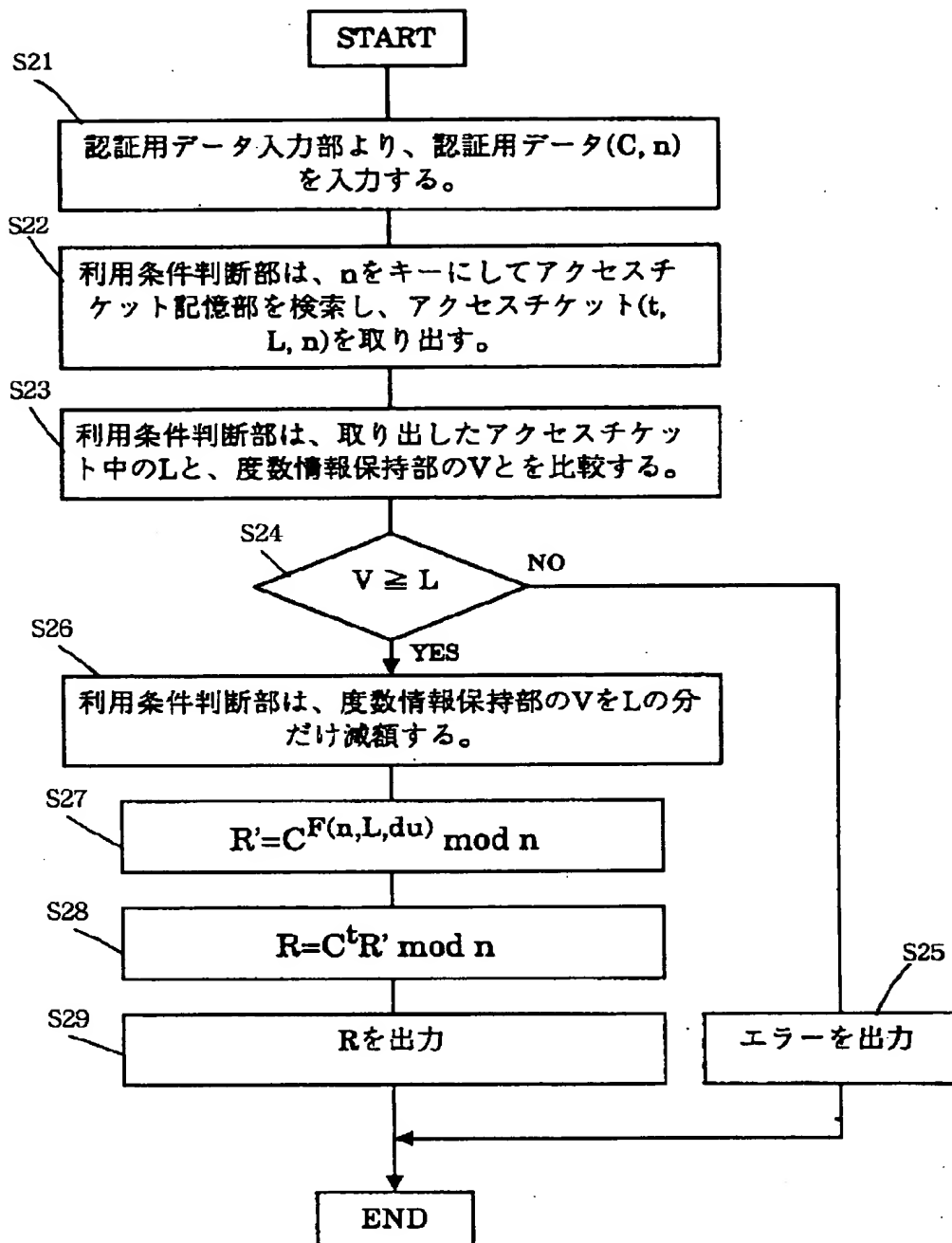
実施例の詳細構成図

【図3】



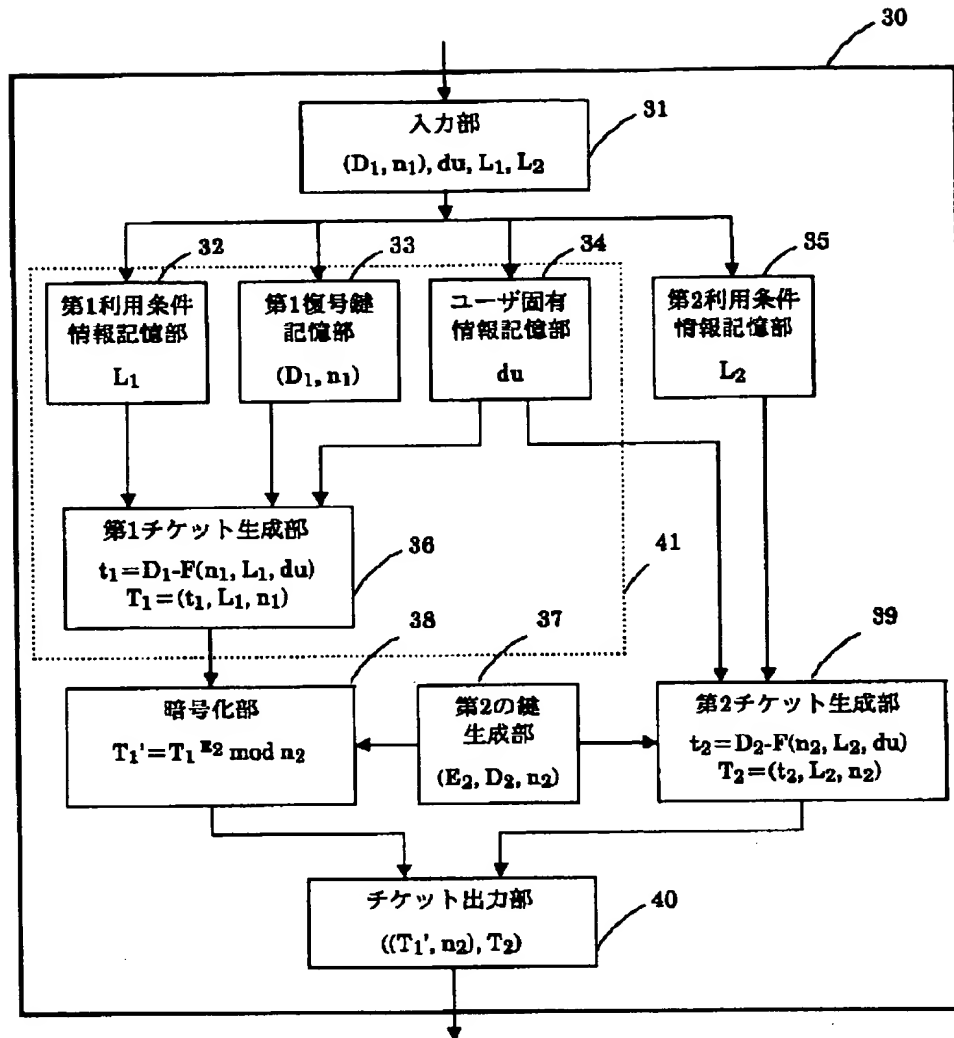
証明データ検証装置における認証用データ生成処理

【図 4】



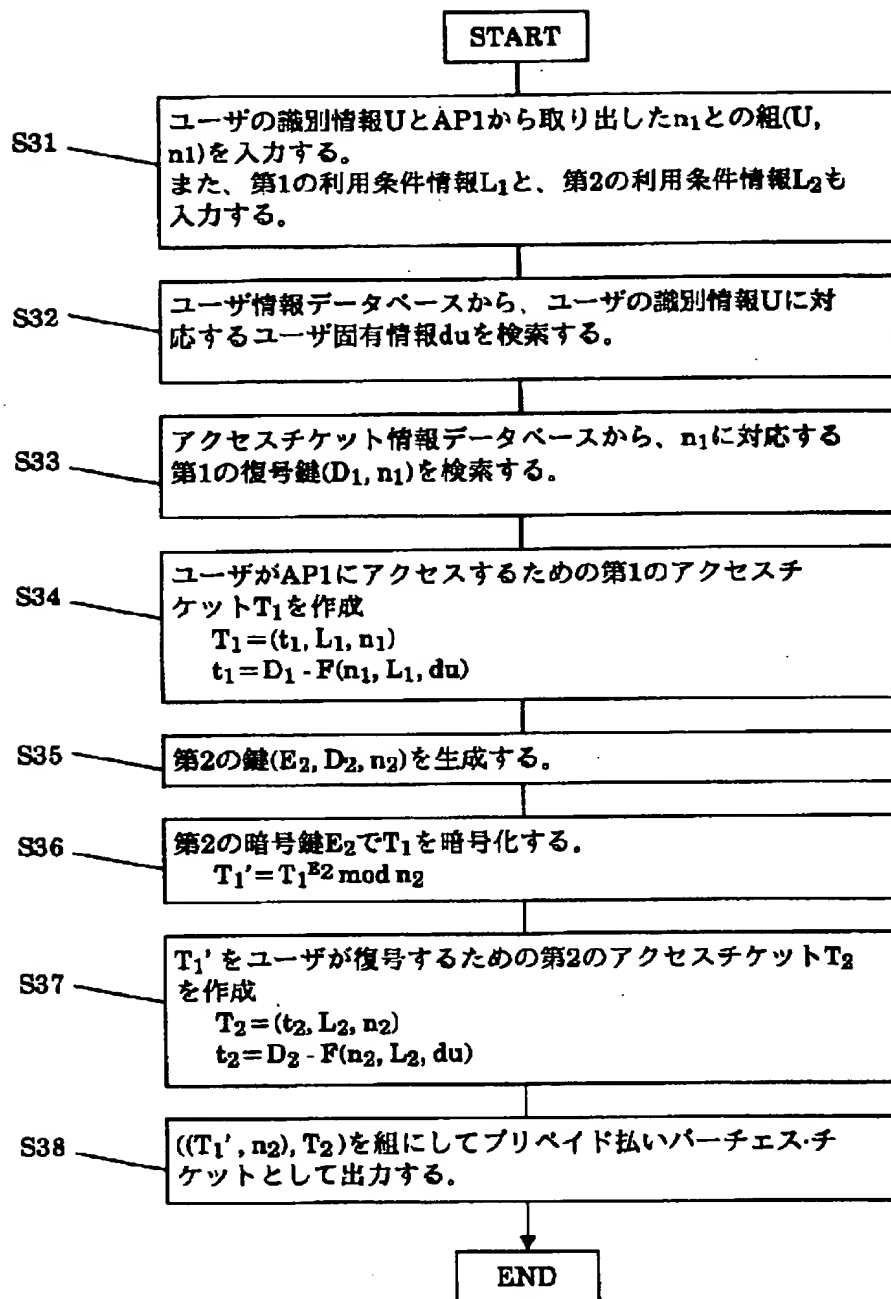
証明データ生成装置における処理

【図5】



証明用補助情報生成装置の構成図

【図6】



プリペイド払いバーチェスチケット作成処理